Resilient control of networked control systems with stochastic denial of service attacks

Article (Accepted Version)

Resilient control of networked control systems with stochastic denial of service attacks

Hongtao Sun[a], Chen Peng,[a,*], Taicheng Yang[a], Hao Zhang[a], Wangli He[b]

[a] *Department of Automation, School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China*

[b] *The Key Laboratory of Advanced Control and Optimization for Chemical Processes, Ministry of Education, East China University of Science and Technology, Shanghai 200237, China*

Abstract

This paper focuses on resilient control of networked control systems (NCSs) under the denial of service (DoS) attacks which is characterized by a Markov process. Firstly, the packets dropout are modeled as Markov process according to the game between attack strategies and defense strategies. Then, an NCS under such game results is modeled as a Markovian jump linear system and four theorems are proved for the system stability analysis and controller design. Finally, a numerical example is used to illustrative the application of these theorems.

Keywords: Networked Control Systems; DoS Attacks; Markovian Process; Resilient Control

1. Introduction

Networked control systems (NCSs) have received an increasing attention in the past decades. Now, NCSs have been widely applied in industrial processes, electric power networks, intelligent transportation and so on ([1, 2, 3, 4]). With the growing of the NCSs, network, as a critical element in an NCS, is vulnerable to cyber-threats which can menace the control systems ([5, 10]). In the presence of network attacks or unreliable links, the separation design of the

*Chen Peng

Email address: c.peng@shu.edu.cn (Chen Peng,)

network security and the networked controller is no longer available. Therefore, the design of NCSs under consideration of network attacks is extremely urgent ([6, 7]). A most common network attack style is so-called denial of service (DoS). DoS attacks usually prevent the information exchange through a large volume invalid data to deliberately consume the network resources. Control problems in the presence of network attacks have been discussed in some recent works, such as in [8, 9, 11, 12]. On the one hand, an attacker would do it best to degrade the performance of the NCSs from the perspective of their own. In the scenario that DoS occurred during the data transmission between sensor and remote estimator with energy constraints, an optimal attack schedules that to maximize the expected average estimation error is studied in [9]. Considering the limitation of attackers, a feedback controller that maximize a given function subjected to safety and power constraints is designed for a class of DoS attack models in [13]. A two-player zero-sum stochastic game is formulated to model the dynamic interactions between a jammer (attacker) and a sensor transmitter (defender) in [14]. On the other hand, the stability of NCS should be guaranteed when attack occurred from the perspective of controller design. For a signal-input remote control system, a control strategy with placing poles method is studied under the periodic DoS attack in [8]. Under a certain condition of frequency and duration of DoS, the input-to-state stability for the closed loop is analyzed in [11]. A hidden Markovian model which is used to describe the attacker jams the control packets stochastically and the stability problem are investigated in [15]. However, there are few works on the stochastic consecutive packets dropout, these issues motivate the current study.

Generally, the attacker's purpose is to prevent the updating of control signal for the DoS attacks. That is to say, packet dropout would occur due to the DoS attacks and induce the instability of the control systems by denying the communication of control signal. Traditionally, the robust control strategies which only consider the worst case of QoS (Quality of Service) are often used to stabilize the NCSs. However, these robust controllers are deemed to lack of flexibility and adaptability. So, more flexible control strategies which can

settle the stability problem of the NCSs with the consideration of the concrete behaviors of packets dropout should be designed. Contributions to this topic in the NCSs have been reported in [17, 18, 19, 20]. The stability and its controller design of networked control systems with both arbitrary and Markovian packet losses are established via a packet-loss depended Lyapunov approach in [16]. For a class of continuous-time and discrete-time Markovian jump linear system (MJLS) with partly unknown transition probabilities, the stability and stabilization problems are investigated in [18]. Without the knowledge of all the transition probabilities, packet-loss-dependent switching controllers which considered both the packet-loss and time delay are designed in [19]. However, network attacks are ignored in the above mentioned works. These motivates the current study.

The objective of this paper is to design a resilient control strategy to resist the DoS attacks for a class of NCSs. Different from the single robust controller, we aim to find a group of controllers to deal with varying degrees of DoS attacks, resiliently. In fact, the packets dropout can be seen as the results of game between attack and defense. However, these results are stochastic and can be described with Markov process. The main contributions of the paper can be summarized as:

(a) Due to the stochastic game between both sides of attack and defense, the packets dropout induced by the DoS attacks is modeled by a Markov process with full or part transition probabilities, and an MJLS model is well constructed to describe the networked control systems under the condition of stochastic noises. This is convenience for us to design the resilient controller for the studied system under the DoS attacks; and

(b) Based on the proposed MJLS model according to the results of game between attack and defense, a stability criterion and a stabilization criterion are established for the system under consideration with the stochastic DoS attacks and stochastic noise. Since the full transition probabilities are not needed, the designed control scheme is resilient to the DoS attacks.

The rest of this paper is organized as follows: In section II, the MJLS model

of the studied system is formulated under consideration of the DoS attacks and the feedback noise; In section III, some results about stochastic stability criteria under network attacks are derived with the full and partial-known transition probabilities; The following section IV shows the numerical simulations to verify the given results; The last section V concludes this paper.

2. Problem Formulation

In this section, the problem of secure control for discrete-time linear system is formulated under consideration of the stochastic characteristic of the DoS attacks.

A typical scenario of an NCS under the DoS attack and the stochastic feedback noise is depicted in Fig. 1. The plant in Fig.1 is

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{1}$$

where $x(t) \in \Re^n$ is the state vector, $u(t) \in \Re^m$ is the control input. A, B are constant matrices with appropriate dimensions.

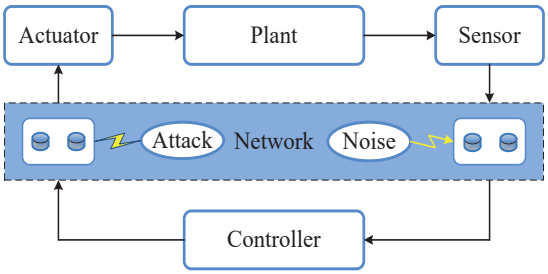

Fig. 1 A scenario of an NCS under the DoS attacks and the stochastic noise

Suppose the control signal $u(t)$ is hold by zero-order-hold style with sampling period T_0. Then the discrete-time model can be represented as

$$x_{\gamma_0}(k+1) = G_{\gamma_0}x(k) + H_{\gamma_0}u(k) \tag{2}$$

where $G_{\gamma_0} = e^{AT_0}$,$H_{\gamma_0} = B\int_0^{T_0} e^{A\tau}d\tau$ and γ_0 represents there is no DoS attack.

In ideal network state, the sensor and control signal can be updated every T_0 time. However, due to the vulnerability of network, the transmission of sensor or control signal is often blocked by an attacker which may cause the denial of service. We consider the scenario that there is an attacker between controller and actuator. Denote γ_i as the subsystem that there are i-consecutive packets dropout for γ_i subsystem. Then, these i-consecutive packets would not be received by actuator and the actuator generate an input that is based on the most recently received control signal until the end of attacks. The details can be seen as Fig.2.

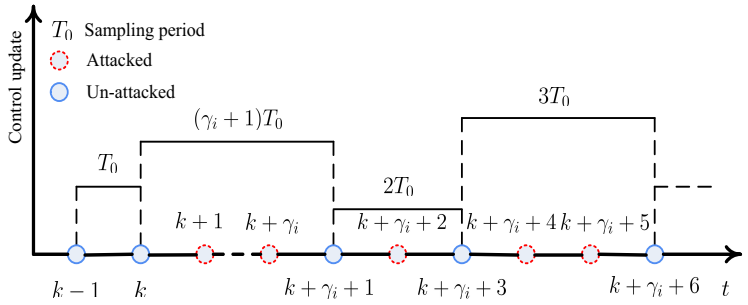

Fig. 2 Control signal update under DoS

When the control packets are jammed, the varying sampling period method can be adopted to obtain the discrete-time system by [21, 22]. So, if there are i-consecutive packets dropout, the forms of discrete-time system are as follows

$$x_{\gamma_i}(k+1) = G_{\gamma_i}x(k) + H_{\gamma_i}u(k) \tag{3}$$

where $G_{\gamma_i} = e^{A(\gamma_i+1)T_0}$,$H_{\gamma_i} = B\int_0^{(\gamma_i+1)T_0} e^{A\tau}d\tau$. And, the subsystem γ_i can jump to the subsystem γ_j in Markov transition probability for all $i, j \in S$.

According to [15] [16], suppose the i take values in set $S = \{1, 2, \cdots, M\}$ which the maximum M represents the energy constraint of attack, then the above attack process with packets dropout can be modeled as Markovian jump linear systems based on the following fact:

Suppose that the attacker adopt attack strategies $A = \{a_1, a_2, \cdots, a_M\}$ and the defender adopt defend strategies $D = \{d_1, d_2, \cdots, d_M\}$, the results between

attack and defense which indicated by packets dropout $S = \{1, 2, \cdots, M\}$ can be seen as stochastic and

Definition 1 : For a given five-element set (Ω, A, D, S, P), packets dropout due to Markov modulated DoS attack takes finite values in $i \in S$ and the transition probabilities are given

$$p_{ij}(a_i, d_j) = Pr(\gamma_j(k+1) = j | \gamma_i(k) = i) \tag{4}$$

where the transition probability represents that packets dropout shift from i to j if attacker adopt attack strategy a_i and the defender adopt defend strategy d_j. Hereafter, the $p_{ij}(a_i, d_j)$ will be denoted as p_{ij} for simplicity.

Thus, two categories of the transition probability matrix are shown

(I) Full-information transition probability matrix which represents these all known games behavior can be obtained completely

$$P = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1M} \\ p_{21} & p_{22} & \cdots & p_{2M} \\ \vdots & \vdots & \vdots & \vdots \\ p_{M1} & p_{M2} & \cdots & p_{MM} \end{pmatrix} \tag{5}$$

where $p_{ij} \geq 0$ and $\sum_{j=1}^{M} p_{ij} = 1$.

(II) Partial-known transition probability matrix which represents only partial games behavior are known can be obtained

$$P = \begin{pmatrix} p_{11} & p_{12} & \mathcal{X} & \cdots & p_{1M} \\ \mathcal{X} & p_{22} & p_{23} & \cdots & \mathcal{X} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{M1} & \mathcal{X} & \mathcal{X} & \cdots & p_{MM} \end{pmatrix} \tag{6}$$

where p_{ij} are known transition probabilities as in (5) and $\mathcal{X}$ are unknown transition probabilities.

Remark 1: If the effect of attack strategy a_i and defense strategy d_j are not clear, we have reason to modeling them to the unknown probability. In

addition, in order to perceived the real-time information of packets dropout, the TCP-based platform with acknowledgment mechanism should be adopted.

To make the proposed model more suitable for practical purpose, the uncertain of state should be considered. Here, the controller including the uncertain of state (refer to [23]) can be designed as the following forms

$$u(k) = K_{\gamma_i} diag[1 + v_{k1}, 1 + v_{k2}, \cdots, 1 + v_{kn}]x(k) \tag{7}$$

where v_{ki} is independent Gaussian white noise for state components with $E[v_{ki}] = 0$, $E[v_{ki}^2] = \sigma^2$ and $E[v_{ki}v_{kj}] = 0$.

Integrating the equations (3) and (7), one has

$$x_{\gamma_i}(k+1) = (G_{\gamma_i} + H_{\gamma_i} K_{\gamma_i} diag[1 + v_{k1}, 1 + v_{k2}, \cdots, 1 + v_{kn}])x(k) \tag{8}$$

Under the controller (7), the following control objective is expected to achieve

Definition 2: System (8) under the attack sequence γ_i is said to be stochastically stable, if, for any initial x_0 and $\gamma_i \in \{0, 1, 2 \cdots, M\}$, the following condition holds:

$$\sum_{k=0}^{\infty} E(\| x(k), \gamma_i \|) < \infty \tag{9}$$

For convenience, the following useful lemma should be pre-presented:

Lemma 1 [24]: The autonomous systems $x(k+1) = A_i x(k)$ with A_i, $i \in \{1, 2, \cdots N\}$ obey a Markovian process are stochastically stable, if and only if there exist a set of symmetric and positive definite matrices P_i satisfying

$$A_i^T \mathcal{P} A_i - P_i < 0 \tag{10}$$

where $\mathcal{P} = \sum_i p_{ij} P_j$.

Remark 2: System (2) represents the condition that there is no DoS attack happened. From the description above, it is easy to know that system (3) involves system (2) as a special case. Because the final result of DoS attacks is the lack of control packets due to network blocked, the actuator channel we only considered in this paper has it certain representativeness. Moreover, both the DoS attacks in control loop and the stochastic noise in feedback loop are considered in this paper, which is different from the aforementioned works in [16, 21].

3. Resilient control under DoS attacks

In this section, four Theorems are provided for stability and stabilization for the studied system with the DoS attacks. In the subsection 3.1, under the case of full-known transition probabilities of DoS attacks, Theorem 1 is provided to judge the stability of the closed-loop system (8), and Theorem 2 is used to solve the resilient controller gain. In the subsection 3.2, under consideration of the case of partial known transition probabilities of the DoS attacks, Theorems 3 and 4 are used to judge the stability and design the resilient controller gain of the closed-loop system (8), respectively.

3.1. Resilient control with full-known transition probabilities

In this subsection, we address the case where the full transition probabilities of the DoS attacks are known in the design of resilient controller for the studied system.

Theorem 1. *For the attack sequence $\gamma_i \in S$ which modulated by Markov transition probability (4), the closed system (8) is stochastic stable if there exist positive definite symmetry matrices $P_i > 0$ such that*

$$[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T \sum_{j=0}^{M} p_{ij}P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] - P_i < 0 \qquad (11)$$

Proof: Let $\gamma_i = i$. Constructing the following attack sequence-dependent Lyapunov function

$$V(x_{\gamma_i}(k)) = x_{\gamma_i}^T(k)P_i x_{\gamma_i}(k) \qquad (12)$$

$$\begin{aligned}
& E[V(x_{\gamma_j}(k+1))|\gamma_i = i] - V(x_{\gamma_i}(k)) \\
= \; & x_{\gamma_j}^T(k+1)\sum_{j=1}^{M} p_{ij}P_j x_{\gamma_j}(k+1) - x_{\gamma_i}^T(k)P_i x_{\gamma_i}(k) \\
= \; & E\{[(G_{\gamma_i} + H_{\gamma_i}K_{\gamma_i}diag[1+v_{k1}, 1+v_{k2}, \cdots, 1+v_{kn}]))x_{\gamma_i}(k)]^T \sum_{j=1}^{M} p_{ij}P_j \\
& [(G_{\gamma_i} + H_{\gamma_i}K_{\gamma_i}diag[1+v_{k1}, 1+v_{k2}, \cdots, 1+v_{kn}]))x_{\gamma_i}(k)]\} - x_{\gamma_i}^T(k)P_i x_{\gamma_i}(k)
\end{aligned}$$

Let $R = diag[1+v_{k1}, 1+v_{k2}, \cdots, 1+v_{kn}])$ which represents the uncertain of state and noticed that $R = R^T$, $E[v_k] = 0$, $D[v_k] = \sigma^2$. As well known, the covariance is usually to describe the dispersion degree of random variables, then, the uncertain of state can be measured by $E(R^T R) = diag[1+\sigma^2, 1+\sigma^2, \cdots, 1+\sigma^2]$. Therefore, for each definite symmetry matrices $P_j > 0$, we compute the expectation for each subsystem j which obey the Markovian transition probabilities as follows

$$\begin{aligned}
& E\{x_{\gamma_i}^T(k)[G_{\gamma_j} + H_{\gamma_j}K_{\gamma_j}diag[1+v_{k1}, 1+v_{k2}, \cdots, 1+v_{kn}])]^T) \sum_{j=1}^{M} p_{ij}P_j \\
& [G_{\gamma_j} + H_{\gamma_j}K_{\gamma_j}diag[1+v_{k1}, 1+v_{k2}, \cdots, 1+v_{kn}])]x_{\gamma_i}(k)\} - x_{\gamma_i}^T(k)P_i x_{\gamma_i}(k) \\
= \; & x_{\gamma_j}^T(k)[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T \sum_{j=1}^{M} p_{ij}P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]x_{\gamma_j}(k) - x_{\gamma_i}^T(k)P_i x_{\gamma_i}(k) \\
= \; & x_{\gamma_i}^T(k)([G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T \sum_{j=1}^{M} p_{ij}P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] - P_i)x_{\gamma_i}(k)
\end{aligned}$$

By Lemma 1, if $[G_{\gamma_j}+(1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T \sum_{j=1}^{M} p_{ij}P_j[G_{\gamma_j}+(1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]-P_i \leq 0$ for all $\gamma_i \in S$ holds, the system is considered as stable.

Let $\alpha = \lambda_{min}\{[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T \sum_{j=1}^{M} p_{ij}P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] - P_i\}$ where $\lambda_{min}\{\star\}$ is the minimum eigenvalue of matrix $\star$, then the following inequality holds

$$E[V(x_{\gamma_j}(k+1))|\gamma_i = i] - V(x_{\gamma_i}) \leq -\alpha x_{\gamma_i}^T(k)x_{\gamma_i}(k) = -\alpha\|x_{\gamma_i}(k)\|^2 \qquad (13)$$

for all $\gamma_i \in S$.

So, for $\forall x_{\gamma_i(k)} \neq 0$

$$\sum_{k=0}^{\infty} E[\|x_{\gamma_i}(k)\|^2|x_0, \gamma_0] \leq \alpha^{-1}E[V(x_{\gamma_0})] < \infty \qquad (14)$$

Combining (9), (13) and (14), the system (8) is stochastic stable.

Proof completed.

Theorem 2. *For the attack sequence $\gamma_i \in S$ which modulated by Markov transition probabilities (4), the closed system (8) is stochastic stable if there exist*

positive definite symmetry matrices $X_i > 0, Y_i > 0$ *such that*

$$\begin{pmatrix} -X_i & * & * & * \\ \sqrt{p_{i1}}G_{\gamma_1}X_1 + (1+\sigma^2)H_{\gamma_1}Y_1 & -X_1 & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ \sqrt{p_{iM}}G_{\gamma_M}X_M + (1+\sigma^2)H_{\gamma_M}Y_M & 0 & 0 & -X_M \end{pmatrix} < 0 \qquad (15)$$

The resilient controller gain with attack sequence γ_i *can be obtained by* $K_{\gamma_i} = Y_i X_i^{-1}$.

Proof: According to the (11), the following inequality is hold by exploiting Lemma 1:

$$\begin{pmatrix} -P_i & * & * & * \\ \sqrt{p_{i1}}P_1(G_{\gamma_1} + (1+\sigma^2)H_{\gamma_1}K_{\gamma_1}) & -P_1 & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ \sqrt{p_{iM}}P_M(G_{\gamma_M} + (1+\sigma^2)H_{\gamma_M}K_{\gamma_M}) & 0 & 0 & -P_M \end{pmatrix} < 0 \qquad (16)$$

Define $X_i = P_i^{-1}$ and pre-and-post multiplying both side of (16) with $diag\{P_i^{-1}, P_1^{-1}, \cdots, P_M^{-1}\}$. Let $X_i = P_i^{-1}$ and $Y_i = K_{\gamma_i}X_i$,we can obtain (15).

Proof completed.

3.2. Resilient control with partial-known transition probabilities

In this subsection, we address the case where the only part known transition probabilities of the DoS attacks are known in the design of resilient controller for the studied system.

For convenience, we first denote the following notations. If the transition probabilities p_{ij} due to attack sequence $\gamma_i \in S$ are known in the ith row, we denote it as

$$P_i^a = \begin{pmatrix} p_{i1} & p_{i2} & \cdots & p_{ij} & \cdots & p_{ip}. \end{pmatrix} \qquad (17)$$

If the transition probabilities p_{ij} due to attack sequence $\gamma_i \in S$ are part known in the ith row, we denote it as

$$P_i^b = \begin{pmatrix} \S_{i1} & \S_{i2} & \cdots & \S_{ij} & \cdots & \S_{iq} \end{pmatrix} \qquad (18)$$

Noted that $P_i^a + P_i^b = P_i$ where the P_i represents all elements in i-th row for probabilities transition matrix P.

Based on the above notations, the following two theorems are derived by use of the Lyapunov theory.

Theorem 3. *For the attack sequence $\gamma_i \in S$ modulated by partial-known Markov transition probabilities (4), the closed-loop system (8) is stochastic stable if there exist positive definite symmetry matrices $P_i > 0$, such that*

$$\begin{aligned}
&[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T \sum_{j\in P_i^a} p_{ij}P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] \\
&- \sum_{j\in P_i^a} p_{ij}P_i < 0 \quad \forall j \in P_i^a \qquad (19)\\
&[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] \\
&-P_i < 0 \quad \forall j \in P_i^b \qquad (20)
\end{aligned}$$

Proof: According to(11) and $\sum_{j=0}^{M-1} P_i = \sum_{j\in P_i^a} p_{ij} + \sum_{j\in P_i^b} p_{ij} = 1$, one has

$$[G_{\gamma_j}+(1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T(\sum_{j\in P_i^a} p_{ij}+\sum_{j\in P_i^b} p_{ij})P_j[G_{\gamma_j}+(1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]-(\sum_{j\in P_i^a} p_{ij}+\sum_{j\in P_i^b} p_{ij})P_i < 0$$

Namely,

$$\begin{aligned}
&[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T \sum_{j\in P_i^a} p_{ij}P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] - \sum_{j\in P_i^a} p_{ij}P_i \\
&+[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T \sum_{j\in P_i^b} p_{ij}P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] - \sum_{j\in P_i^b} p_{ij}P_i < 0
\end{aligned}$$

Let

$$\begin{aligned}
\Psi_i^a &= [G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T \sum_{j\in P_i^a} p_{ij}P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] - \sum_{j\in P_i^a} p_{ij}P_i \\
\Psi_i^b &= [G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T \sum_{j\in P_i^b} p_{ij}P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] - \sum_{j\in P_i^b} p_{ij}P_i
\end{aligned}$$

and $\Psi_i = \Psi_i^a + \Psi_i^b$. At the same time, Ψ_i^b can be re-stated as

$$\begin{aligned}\Psi_i^b &= [G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T \sum_{j\in P_i^b} p_{ij}P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] - \sum_{j\in P_i^b} p_{ij}P_i \\ &= \sum_{j\in P_i^b} p_{ij}[[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] - P_i]\end{aligned}$$

If $\Psi_i < 0$ holds, thus

$$\begin{aligned}\Psi_i^a &= [G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T \sum_{j\in P_i^a} p_{ij}P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] - \sum_{j\in P_i^a} p_{ij}P_i < 0 \\ \Psi_i^b &= \sum_{j\in P_i^b} p_{ij}[[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] - P_i] < 0\end{aligned}$$

Because $\sum_{j\in P_i^b} p_{ij} > 0$, for $\forall j \in P_i^b$:

$$[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}]^T P_j[G_{\gamma_j} + (1+\sigma^2)H_{\gamma_j}K_{\gamma_j}] - P_i < 0$$

Proof completed.

Theorem 4. *For the attack sequence $\gamma_i \in S$ which modulated by the partial known Markov transition probabilities (6), the closed-loop system (8) is stochastic stable if there exist positive definite symmetry matrices $X_i > 0, Y_i > 0$ such that*

$$\begin{pmatrix} -\sum_{j\in P_i^a} \sqrt{p_{ij}}X_i & * & * & * \\ \sqrt{p_{i1}}G_{\gamma_1}X_1 + (1+\sigma^2)H_{\gamma_1}Y_1 & -X_1 & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ \sqrt{p_{ip}}G_{\gamma_p}X_p + (1+\sigma^2)H_{\gamma_p}Y_p & 0 & 0 & -X_p \end{pmatrix} < 0 \quad \forall j \in P_i^a \qquad (21)$$

$$\begin{pmatrix} -X_i & * & * & * \\ G_{\gamma_1}X_j + (1+\sigma^2)H_{\gamma_1}Y_1 & -X_1 & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ G_{\gamma_q}X_q + (1+\sigma^2)H_{\gamma_q}Y_q & 0 & 0 & -X_q \end{pmatrix} < 0 \quad \forall j \in P_i^b. \qquad (22)$$

The resilient controller gain with attack sequence γ_i can be obtained by $K_{\gamma_i} = Y_i X_i^{-1}$.

Proof: According to the (19) and (20), the following inequalities are hold by exploiting Schur complement lemma

$$\begin{pmatrix} -\sum\limits_{j\in P_i^a}\sqrt{p_{ij}}P_i & * & * & * \\ \sqrt{p_{i1}}P_1(G_{\gamma_1}+(1+\sigma^2)H_{\gamma_1}K_{\gamma_1}) & -P_1 & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ \sqrt{p_{ip}}P_p(G_{\gamma_p}+(1+\sigma^2)H_{\gamma_p}K_{\gamma_p}) & 0 & 0 & -P_p \end{pmatrix} < 0 \quad \forall j \in P_i^a$$

$$\begin{pmatrix} -P_i & * & * & * \\ P_1(G_{\gamma_1}+(1+\sigma^2)H_{\gamma_1}K_{\gamma_1}) & -P_1 & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ P_q(G_{\gamma_q}+(1+\sigma^2)H_{\gamma_q}K_{\gamma_q}) & 0 & 0 & -P_q \end{pmatrix} < 0 \quad \forall j \in P_i^b$$

Similar to Theorem 2, define $X_i = P_i^{-1}$ and pre-and-post multiplying both side of (21) and (22) with $diag\{P_i^{-1}, P_j^{-1}, \cdots, P_p^{-1}\}$ and $diag\{P_i^{-1}, P_j^{-1}, \cdots, P_q^{-1}\}$, respectively. Let $X_i = P_i^{-1}$ and $Y_i = K_{\gamma_i}X_i$, we can obtain (21) and (22).

Proof completed.

4. An example

In this section, under three different DoS attack scenes, a numerical example is given to show the validity of the proposed theoretical results.

Considering the continue-time system in [16]

$$\dot{x}(t) = \begin{pmatrix} -1 & 0 & -0.5 \\ 1 & -0.5 & 0 \\ 0 & 0 & 0.5 \end{pmatrix} x(t) + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} u(t) \tag{23}$$

Suppose there is DoS attacks in the networked control of the system (23) with the attack sequence $\gamma_i \in \{1T_0, 2T_0, 3T_0\}$, where $T_0 = 0.1s$. Based on Eq.(3), the system parameters under the newly sampling period $\{2T_0, 3T_0, 4T_0\}$ are given as

$$A_1 = \begin{pmatrix} 0.8187 & 0 & -0.0955 \\ 0.1772 & 0.9048 & -0.0094 \\ 0 & 0 & 1.1052 \end{pmatrix} \quad B_1 = \begin{pmatrix} -0.0025 \\ -0.0001 \\ 0.1025 \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 0.7408 & 0 & -0.1404 \\ 0.2398 & 0.8607 & -0.0204 \\ 0 & 0 & 1.1618 \end{pmatrix} \quad B_2 = \begin{pmatrix} -0.0215 \\ -0.0021 \\ 0.3237 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 0.6703 & 0 & -0.1837 \\ 0.2968 & 0.8187 & -0.0353 \\ 0 & 0 & 1.2214 \end{pmatrix} \quad B_3 = \begin{pmatrix} -0.0377 \\ -0.0048 \\ 0.4428 \end{pmatrix}$$

Suppose there exist attack strategies $A = \{a_1, a_2, a_3\}$ and defend strategies $D = \{d_1, d_2, d_3\}$. The transition probabilities matrix of Markovian packets dropout which caused by two sides of attack and defend may be follow the three cases for the system (3) with the above given parameters.

Case I: DoS with full-known transition probabilities

If the transition probabilities for all attack strategy a_i and defend strategy d_j can be perceived, the full-information transition probabilities of packet dropout due to Markov modulated DoS attack is given by

$$P = \begin{pmatrix} 0.3 & 0.4 & 0.3 \\ 0.4 & 0.2 & 0.4 \\ 0.5 & 0.1 & 0.4 \end{pmatrix}$$

By Theorem 1, the group of resilient controller gains for each subsystem can be obtained

$$\begin{aligned} K_1 &= [0.1473, 0.0281, -2.0853] \\ K_2 &= [0.2405, 0.0599, -2.1004] \\ K_3 &= [0.2774, 0.0196, -2.1109] \end{aligned} \tag{24}$$

Let the initial state as $x_0 = [1.6, -1.2, -0.4]^T$. Without loss of generality, we adopt the $2T_0$ as the current state of packet dropout. The state response under Markov modulated DoS attack is shown in Fig.3.

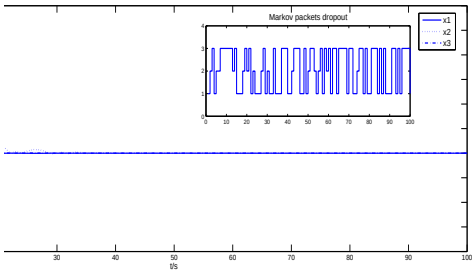

Fig. 3 State response under full-information Markov attack with controller gains (24)

Clearly, if full-information transition probabilities which depend on attack strategies and defend strategies are given, the designed resilient controller with the gains (24) is effective for arbitrary transition probabilities $p_{ij} \in [0, 1]$ of packets dropout.

Case II: DoS with part-known transition probabilities

If not all transition probabilities for all attack strategy a_i and defend strategy d_j can be perceived, the partial-known transition probabilities of packets dropout under Markov modulated DoS attack are given by

$$P = \begin{pmatrix} ? & 0.7 & ? \\ ? & 0.8 & ? \\ 0.75 & ? & ? \end{pmatrix}$$

We set the same initial states and adopt the same controller gains (24) in **Case I**, the state response under Markov modulated DoS is shown in Fig.4.

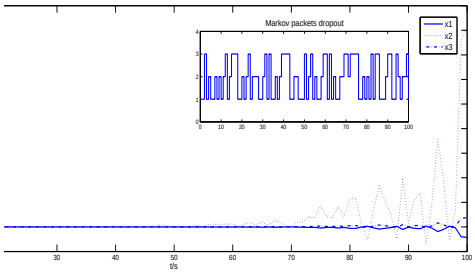

Fig. 4 State responses under partial-known DoS attacks with the controller gains (24)

Comparing Fig.3 and Fig.4, one can see that the system (3) is unstable if we some transition probabilities are unknown to us. This is tally with the actual situation. If we blind to the attackers' behavior, the designed controller are doom to failure which motivated our to seek a new control strategies. By Theorem 3, the controller gains can be obtained

$$\begin{aligned} K_1 &= [0.2771, 0.1524, -2.6394] \\ K_2 &= [10.7303, 5.4914, -2.1557] \\ K_3 &= [1.3862, 1.1260, -3.0455] \end{aligned} \tag{25}$$

With the same initial state in **case I** and the new resilient controller gains (25), the state responses is shown in Fig.5.

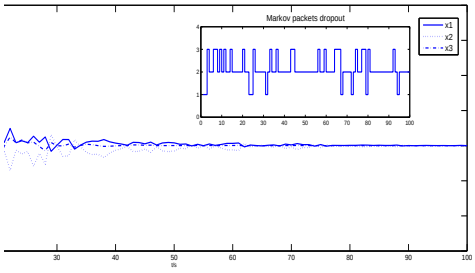

Fig. 5 State responses with the controller gains (25)

It is noted that the resilient controller gains (25) can stabilize the NCS but

less effective than the resilient controller gains (24). In fact, there are not always efficient for arbitrary partial-known transition probability except that the known probabilities are large enough. This implies that: the more knowledge about two sides of attack and defense, the efficient for our designed resilient controller.

5. Conclusion

In this paper, a resilient control problem of networked control systems under DoS attacks has been addressed. When the attacker jam the control packets from the actuator, the discrete time Markovian jump linear system has been used to model the process of packets dropout. Considering the concealment of attacks and using the Lyapunov method and LMIs technique, the resilient control schemes under full or partial known transition probabilities have been well investigated. Moreover, the stochastic noise in feedback loop has also been considered. Although the proposed control strategy shows the 'resilience' to different degrees of packets dropout due to DoS attacks, there are no compensation strategy to compensate the packets dropout which reflect the 'passivity' of our proposed control strategy. How to consider the resilient control for NCSs without assuming the DoS attack satisfying some predefined stochastic distributions and how to compensate these packets dropout in the scene of DoS attacks are left for our future study.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grants 61273114,61673255, 61633016 and 61573141, the International Corporation Project of Shanghai Science and Technology Commission under Grants 14510722500 and 15220710400, the Science and Technology Commission of Shanghai Municipality under Grant 15JC1401900.

References

[1] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, C.-F. Covrig, A survey on the critical issues in smart grid technologies, Renewable and Sustainable Energy Reviews 54 (2016) 396–405.

[2] S. Liu, X. P. Liu, A. E. Saddik, Modeling and distributed gain scheduling strategy for load frequency control in smart grids with communication topology changes., Isa Transactions 53 (2) (2014) 454–461.

[3] C. Peng, J. Zhang, Delay-distribution-dependent load frequency control of power systems with probabilistic interval delays, IEEE Transactions on Power Systems 31 (4) (2016) 3309-3317.

[4] S. Deng, D. Yue, X. Fu, A. Zhou, Security risk assessment of cyber physical power system based on rough set and gene expression programming, IEEE/CAA Journal of Automatica Sinica, 2 (4) (2015) 431–439.

[5] H. Sandberg, S. Amin, K. Johansson, Cyberphysical security in networked control systems: an introduction to the issue, IEEE Control Systems, 35 (1) (2015) 20–23.

[6] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, Challenges for securing cyber physical systems, in: Workshop on future directions in cyber-physical systems security (2009) 1–7.

[7] X.-P. Xie, D. Yue, C. Peng, Relaxed fuzzy control synthesis of nonlinear networked systems under unreliable communication links, Applied Soft Computing. 41 (2016) 180C191

[8] H. S. Foroush, S. Martínez, On single-input controllable linear systems under periodic dos jamming attacks, arXiv preprint arXiv:1209.4101.

[9] H. Zhang, P. Cheng, L. Shi, J. Chen, Optimal denial-of-service attack scheduling with energy constraint, IEEE Transactions on Automatic Control, 60 (11) (2015) 3023–3028.

[10] C. Peng, Q.-L. Han, On designing a novel self-triggered sampling scheme for networked control systems with data losses and communication delays, IEEE Transaction on Industrial Electronics, 63 (2) (2016) 1293–1248

[11] C. De Persis, P. Tesi, Input-to-state stabilizing control under denial-of-service, IEEE Transactions on Automatic Control, 60 (11) (2015) 2930–2944.

[12] A. Gupta, C. Langbort, T. Basar, Optimal control in the presence of an intelligent jammer with limited actions, in: The 49th IEEE Conference on Decision and Control (CDC), (2010) 1096–1101.

[13] S. Amin, A. A. Cárdenas, S. S. Sastry, Safe and secure networked control systems under denial-of-service attacks, in: Hybrid Systems: Computation and Control, Springer, (2009) 31–45.

[14] S. Liu, P. X. Liu, A. E. Saddik, A stochastic game approach to the security issue of networked control systems under jamming attacks, Journal of the Franklin Institute 351 (9) (2014) 4570–4583.

[15] G. K. Befekadu, V. Gupta, P. J. Antsaklis, Risk-sensitive control under markov modulated denial-of-service (dos) attack strategies, IEEE Transactions on Automatic Control, 60 (12) (2015) 3299–3304.

[16] J. Xiong, J. Lam, Stabilization of linear systems over networks with bounded packet loss, Automatica 43 (1) (2007) 80–87.

[17] C. Peng, J. Zhang, Event-triggered output-feedback H_∞ control for networked control systems with time-varying sampling, IET Control Theory and Application, 9 (9)(2015) 1384-1391

[18] L. Zhang, E.-K. Boukas, Stability and stabilization of markovian jump linear systems with partly unknown transition probabilities, Automatica 45 (2) (2009) 463–468.

[19] X. Ye, S. Liu, P. X. Liu, Modelling and stabilisation of networked control system with packet loss and time-varying delays, Control Theory & Applications 4 (6) (2010) 1094–1100.

[20] X. Yin, D. Yue, S. Hu, C. Peng, Y. Xue, Model-based event-triggered predictive control for networked systems with data dropout, SIAM Journal on Control and Optimization 54 (2) (2016) 567–586.

[21] S. Liu, X. P. Liu, A. El Saddik, S. Islam, Modeling and stochastic control of networked control system with packet losses, in: IEEE, Instrumentation and Measurement Technology Conference (I&MTC), (2011) 1–5.

[22] Z. Wang, H. Sun, Z. Xinguo, Multi-rate control and pole assignment for a single closed-loop in networked multi-rate control system, in: The 27th Chinese Control and Decision Conference (CCDC), (2015) 6017–6021.

[23] G. Gu, L. Qiu, Networked stabilization of multi-input systems with channel resource allocation, in: Proceedings of the 17th IFAC World Congress, (2008) 625–630.

[24] E.-K. Boukas, Stochastic switching systems: analysis and design, Springer Science & Business Media, 2007.